Amendments to the Claims

Claim 1 (original): A computer program product for providing end-to-end protection for datagrams in a computer networking environment, the computer program product embodied on one or more computer-readable media and comprising computer-readable program code means for independently securing each of a plurality of network segments that comprise a network path from a datagram originator to a datagram destination, while each of one or more gateways in the network path retains cleartext access to datagrams sent on the network path.

Claim 2 (original): A computer program product for providing end-to-end protection for datagrams in a computer networking environment, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for protecting each of a plurality of network segments that comprise a network path from a datagram originator to a datagram destination, further comprising:

computer-readable program code means for establishing a first protected network segment from the datagram originator to a first gateway in the network path;

computer-readable program code means for cascading zero or more protected gateway-to-gateway segments from the first gateway to each of zero or more successive gateways in the network path; and

computer-readable program code means for cascading a last protected network segment from a final one of the gateways to the datagram destination, wherein the final gateway may be identical to the first gateway if no gateway-to-gateway segments are required,

wherein the first gateway and each of the zero or more successive gateways retains cleartext access to datagrams sent on the network path.

Claim 3 (original): The computer program product according to Claim 2, wherein the computer-readable program code means for establishing and the computer-readable program code means for cascading further comprise computer-readable program code means for establishing security associations which use strong cryptographic techniques.

Claim 4 (original): The computer program product according to Claim 3, wherein the strong cryptographic techniques used for the security associations are provided by protocols known as Internet Key Exchange and IP (Internet Protocol) Security Protocol.

Claim 5 (original): The computer program product according to Claim 2, wherein the computer-readable program code means for cascading further comprises computer-readable program code means for using identifying information from the first protected network segment as identifying information of the protected gateway-to-gateway segments and the protected final network segment.

Claim 6 (original): The computer program product according to Claim 5, wherein the identifying information further comprises addresses of the datagram originator and the datagram destination.

Claim 7 (original): The computer program product according to Claim 6, wherein the identifying information further comprises a protocol identification and a port number used for the first protected network segment.

Claim 8 (original): The computer program product according to Claim 4, wherein the datagram originator and the gateways that perform the computer-readable program code means for cascading each act in an IKE initiator role.

Claim 9 (original): The computer program product according to Claim 2, wherein the datagram originator and the gateways that perform the computer-readable program code means for cascading each act as in an initiator role for a protocol known as Internet Key Exchange.

Claim 10 (original): The computer program product according to Claim 5 or Claim 6, wherein the identifying information is copied from an inbound side of each gateway to an outbound side of that gateway.

Claim 11 (original): The computer program product according to Claim 2, wherein any of the gateways may perform services on the cleartext datagram.

Claim 12 (original): The computer program product according to Claim 2, wherein operation of the computer-readable program code means for cascading may be selectively enabled for any particular network path.

Claim 13 (original): The computer program product according to Claim 12, wherein the selective enablement occurs by setting a cascading-enabled flag for the first protected network segment, and wherein datagrams sent on the network path are not protected using cascaded tunnels when the computer-readable program code means for cascading is disabled.

Claim 14 (original): The computer program product according to Claim 5, wherein the identifying information may be altered by zero or more of the gateways.

Claim 15 (original): A system for providing end-to-end protection for datagrams in a computer networking environment, the system comprising means for independently securing each of a plurality of network segments that comprise a network path from a first computer to a second computer, wherein a datagram originator at the first computer sends at least one datagram to a datagram destination at the second computer, while each of one or more gateways in the network path retains cleartext access to datagrams sent on the network path.

Claim 16 (original): A system for providing end-to-end protection for datagrams in a computer networking environment, comprising:

means for protecting each of a plurality of network segments that comprise a network path from a datagram originator to a datagram destination, further comprising:

means for establishing a first protected network segment from the datagram originator to a first gateway in the network path;

means for cascading zero or more protected gateway-to-gateway segments from the first gateway to each of zero or more successive gateways in the network path; and

means for cascading a last protected network segment from a final one of the gateways to the datagram destination, wherein the final gateway may be identical to the first gateway if no gateway-to-gateway segments are required,

wherein the first gateway and each of the zero or more successive gateways retains cleartext access to datagrams sent on the network path.

Claim 17 (original): The system according to Claim 16, wherein the means for establishing and the means for cascading further comprise means for establishing security associations which use strong cryptographic techniques.

Claim 18 (original): The system according to Claim 17, wherein the strong cryptographic techniques used for the security associations are provided by protocols known as Internet Key Exchange and IP (Internet Protocol) Security Protocol.

Claim 19 (original): The system according to Claim 16, wherein the means for cascading further comprises means for using identifying information from the first protected network segment as identifying information of the protected gateway-to-gateway segments and the protected final network segment.

Claim 20 (original): The system according to Claim 19, wherein the identifying information further comprises addresses of the datagram originator and the datagram destination.

Claim 21 (original): The system according to Claim 20, wherein the identifying information further comprises a protocol identification and a port number used for the first protected network segment.

Claim 22 (original): The system according to Claim 18, wherein the datagram originator and the gateways that perform the means for cascading each act in an IKE initiator role.

Claim 23 (original): The system according to Claim 16, wherein the datagram originator and the gateways that perform the means for cascading each act as in an initiator role for a protocol known as Internet Key Exchange.

Claim 24 (original): The system according to Claim 19 or Claim 20, wherein the identifying information is copied from an inbound side of each gateway to an outbound side of that gateway.

Claim 25 (original): The system according to Claim 16, wherein any of the gateways may perform services on the cleartext datagram.

Claim 26 (original): The system according to Claim 16, wherein operation of the means for cascading may be selectively enabled for any particular network path.

Claim 27 (original): The system according to Claim 26, wherein the selective enablement occurs by setting a cascading-enabled flag for the first protected network segment, and wherein datagrams sent on the network path are not protected using cascaded tunnels when the means for cascading is disabled.

Claim 28 (original): The system according to Claim 19, wherein the identifying information may be altered by zero or more of the gateways.

Claim 29 (original): A method of providing end-to-end protection for datagrams in a computer networking environment, by independently securing each of a plurality of network segments that comprise a network path from a first computer to a second computer, wherein a datagram originator at the first computer sends at least one datagram to a datagram destination at the second computer, while each of one or more gateways in the network path retains cleartext access to datagrams sent on the network path.

Claim 30 (original): A method of providing end-to-end protection for datagrams in a computer networking environment, comprising steps of:

protecting each of a plurality of network segments that comprise a network path from a datagram originator to a datagram destination, further comprising steps of:

establishing a first protected network segment from the datagram originator to a first gateway in the network path;

cascading zero or more protected gateway-to-gateway segments from the first gateway to each of zero or more successive gateways in the network path; and

cascading a last protected network segment from a final one of the gateways to the datagram destination, wherein the final gateway may be identical to the first gateway if no gateway-to-gateway segments are required,

wherein the first gateway and each of the zero or more successive gateways retains cleartext access to datagrams sent on the network path.

Claim 31 (original): The method according to Claim 30, wherein the establishing step and the cascading step further comprise the step of establishing security associations which use strong cryptographic techniques.

Claim 32 (original): The method according to Claim 31, wherein the strong cryptographic techniques used for the security associations are provided by protocols known as Internet Key Exchange and IP (Internet Protocol) Security Protocol.

Claim 33 (original): The method according to Claim 30, wherein the cascading step further comprises the step of using identifying information from the first protected network segment as identifying information of the protected gateway-to-gateway segments and the protected final network segment.

Claim 34 (original): The method according to Claim 33, wherein the identifying information further comprises addresses of the datagram originator and the datagram destination.

Claim 35 (original): The method according to Claim 34, wherein the identifying information further comprises a protocol identification and a port number used for the first protected network segment.

Claim 36 (original): The method according to Claim 32, wherein the datagram originator and the gateways that perform the cascading step each act in an IKE initiator role.

Claim 37 (original): The method according to Claim 30, wherein the datagram originator and the gateways that perform the cascading step each act as in an initiator role for a protocol known as Internet Key Exchange.

Claim 38 (original): The method according to Claim 33 or Claim 34, wherein the identifying information is copied from an inbound side of each gateway to an outbound side of that gateway.

Claim 39 (original): The method according to Claim 30, wherein any of the gateways may perform services on the cleartext datagram.

Claim 40 (original): The method according to Claim 30, wherein operation of the cascading step may be selectively enabled for any particular network path.

Claim 41 (original): The method according to Claim 40, wherein the selective enablement occurs by setting a cascading-enabled flag for the first protected network segment, and wherein datagrams sent on the network path are not protected using cascaded tunnels when the cascading step is disabled.

Claim 42 (original): The method according to Claim 33, wherein the identifying information may be altered by zero or more of the gateways.

Claim 43 (new): A computer program product for providing end-to-end protection for datagrams in a computer networking environment, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for protecting each of a plurality of network segments that comprise a network path from a datagram originator to a datagram destination, further comprising:

computer-readable program code means for establishing a first protected network segment from the datagram originator to a first gateway in the network path;

computer-readable program code means for cascading one or more protected gateway-to-gateway segments from the first gateway to each of one or more successive gateways in the network path, using identifying information from the first protected network segment as identifying information of the protected gateway-to-gateway segments, wherein the identifying information is copied from an inbound side of each gateway to an outbound side of that gateway; and

computer-readable program code means for cascading a last protected network segment from a final one of the gateways to the datagram destination, using identifying information from the first protected network segment as identifying information of the protected final network segment, wherein the identifying information is copied from an inbound side of each gateway to an outbound side of that gateway,

wherein the first gateway and each of the one or more successive gateways retains cleartext access to datagrams sent on the network path.

Claim 44 (new): A system for providing end-to-end protection for datagrams in a computer networking environment, comprising:

means for protecting each of a plurality of network segments that comprise a network path from a datagram originator to a datagram destination, further comprising:

means for establishing a first protected network segment from the datagram originator to a first gateway in the network path;

means for cascading one or more protected gateway-to-gateway segments from the first gateway to each of zero or more successive gateways in the network path, using identifying information from the first protected network segment as identifying information of the protected gateway-to-gateway segments, wherein the identifying information is copied from an inbound side of each gateway to an outbound side of that gateway; and

means for cascading a last protected network segment from a final one of the gateways to the datagram destination, using identifying information from the first protected network segment as identifying information of the protected final network segment, wherein the identifying information is copied from an inbound side of each gateway to an outbound side of that gateway,

wherein the first gateway and each of the one or more successive gateways retains cleartext access to datagrams sent on the network path.

Claim 45 (new): A method of providing end-to-end protection for datagrams in a computer networking environment, comprising steps of:

protecting each of a plurality of network segments that comprise a network path from a datagram originator to a datagram destination, further comprising steps of:

establishing a first protected network segment from the datagram originator to a first gateway in the network path;

cascading one or more protected gateway-to-gateway segments from the first gateway to each of zero or more successive gateways in the network path, using identifying information from the first protected network segment as identifying information of the protected gateway-to-gateway segments, wherein the identifying information is copied from an inbound side of each gateway to an outbound side of that gateway; and

cascading a last protected network segment from a final one of the gateways to the datagram destination, using identifying information from the first protected network segment as identifying information of the protected final network segment, wherein the identifying information is copied from an inbound side of each gateway to an outbound side of that gateway,

wherein the first gateway and each of the one or more successive gateways retains cleartext access to datagrams sent on the network path.